

Optimal Toffoli Implementation

Abdullah Almanei

September 9, 2026

0.1 Overview

This blueprint documents the lower bound for implementing doubly-controlled one-qubit gates using arbitrary two-qubit gates and its specialization to the Toffoli gate. Sections 3–7 formalize the characterization of those $CC(U)$ gates admitting a decomposition with at most four two-qubit factors. The final section combines that lower bound for $U = X$ with an explicit five-gate controlled-square-root construction.

Every theorem in this focused repository is proved without `sorry` or `native_decide`. The final theorem’s axiom closure is exactly `[propext, Classical.choice, Quot.sound]`.

0.2 Section 3: The conditions on the eigenvalues

Lemma 1. *Suppose u_0, u_1 are complex numbers with $|u_0| = |u_1| = 1$. An 8×8 unitary U commutes with $\text{Diag}(u_0, u_1) \otimes I_2 \otimes I_2$ if and only if either $u_0 = u_1$ or $U = |0\rangle\langle 0| \otimes V_{00} + |1\rangle\langle 1| \otimes V_{11}$ for some 4×4 unitaries V_{00}, V_{11} .*

Proof. Decompose U into a 2×2 block matrix of 4×4 submatrices $U = |0\rangle\langle 0| \otimes V_{00} + |0\rangle\langle 1| \otimes V_{01} + |1\rangle\langle 0| \otimes V_{10} + |1\rangle\langle 1| \otimes V_{11}$. Similarly decompose $\text{Diag}(u_0, u_1) \otimes I_2 \otimes I_2$ as a block-diagonal matrix with blocks $u_0 \cdot I_4$ and $u_1 \cdot I_4$. Compute UW and WU and compare blocks: commutativity forces $u_1 \cdot V_{01} = u_0 \cdot V_{01}$ and $u_0 \cdot V_{10} = u_1 \cdot V_{10}$. When $u_0 \neq u_1$, scalar cancellation implies $V_{01} = V_{10} = 0$, giving the block-diagonal form. Unitarity of U then forces V_{00} and V_{11} to be individually unitary. The converse is straightforward. $\square$

Lemma 2. *Suppose u_0, u_1 are complex numbers with $|u_0| = |u_1| = 1$. There exist 2×2 unitaries P, Q such that the eigenvalues of $P \otimes Q$ are $\{1, 1, u_0, u_1\}$ (as a multiset, up to permutation) if and only if either $u_0 = u_1$ or $u_0 u_1 = 1$.*

Proof. (Forward direction.) Diagonalize P and Q via the spectral theorem to write $P = V_P D_P V_P^\dagger$ and $Q = V_Q D_Q V_Q^\dagger$. The eigenvalues of $P \otimes Q$ are the pairwise products of eigenvalues of P and Q . These four products must be a permutation of $\{1, 1, u_0, u_1\}$. Exhaustive case analysis over all 24 permutations of four elements shows each case yields either $u_0 = u_1$ or $u_0 u_1 = 1$.

(Backward direction.) If $u_0 = u_1$, take $P = \text{Diag}(1, u_1)$ and $Q = I_2$. If $u_0 u_1 = 1$, take $P = \text{Diag}(1, u_0)$ and $Q = \text{Diag}(1, u_1)$ with a suitable diagonalizing unitary. $\square$

Lemma 3. *Suppose u_0, u_1 are complex numbers with $|u_0| = |u_1| = 1$. There exist a 2×2 unitary P and complex numbers c, d such that the eigenvalues of $(I_2 \otimes P) \cdot C(\text{Diag}(u_0, u_1))$ are $\{c, c, d, d\}$ (each with multiplicity two) if and only if either $u_0 = u_1$ or $u_0 u_1 = 1$. Here $C(\text{Diag}(u_0, u_1))$ denotes the controlled- $\text{Diag}(u_0, u_1)$ gate.*

Proof. (Forward direction.) Rewrite $(I_2 \otimes P) \cdot C(\text{Diag}(u_0, u_1))$ as the direct sum $P \oplus (P \cdot \text{Diag}(u_0, u_1))$. Diagonalize P and $P \cdot \text{Diag}(u_0, u_1)$ separately via the spectral theorem. The eigenvalues of the direct sum are related by a permutation to those of $\text{Diag}(c, d, c, d)$. Exhaustive case analysis on all 24 permutations of four eigenvalues: if both eigenvalues of P equal the same value c , then P is a scalar multiple of the identity, and a cancellation argument forces $u_0 = u_1$. In the remaining cases, a determinant argument using $\det(AB) = \det(A) \cdot \det(B)$ yields $u_0 u_1 = 1$.

(Backward direction.) If $u_0 = u_1$, take $P = I_2$. If $u_0 u_1 = 1$, take $P = \text{Diag}(1, u_0)$. $\square$

0.3 Section 4: Four key building blocks

Lemma 4. Suppose u_0, u_1 are complex numbers with $|u_0| = |u_1| = 1$. There exist 4×4 unitary matrices U, V and 2×2 unitary matrices P_0, P_1, Q_0, Q_1 such that

$$|0\rangle\langle 0| \otimes U(P_0 \otimes Q_0)V + |1\rangle\langle 1| \otimes U(P_1 \otimes Q_1)V = CC(\text{Diag}(u_0, u_1))$$

if and only if either $u_0 = u_1$ or $u_0 u_1 = 1$.

Proof. Forward direction: decompose $CC(\text{Diag}(u_0, u_1))$ via direct sum into $|0\rangle\langle 0| \otimes I_4 \oplus |1\rangle\langle 1| \otimes C(\text{Diag}(u_0, u_1))$. The hypothesis forces $U(P_0 \otimes Q_0)V = I_4$ and $U(P_1 \otimes Q_1)V = C(\text{Diag}(u_0, u_1))$. Combining yields $\text{Diag}(1, 1, u_0, u_1) = U((P_1 P_0^\dagger) \otimes (Q_1 Q_0^\dagger))U^\dagger$, a similarity relation on a tensor product of 2×2 unitaries. Apply Lemma 3.2 to conclude $u_0 = u_1$ or $u_0 u_1 = 1$.

Reverse direction: if $u_0 = u_1$, take $U = V = I_4$ and appropriate diagonal witnesses. If $u_0 u_1 = 1$, use CNOT-based witnesses. $\square$

Lemma 5. Suppose u_0, u_1 are complex numbers with $|u_0| = |u_1| = 1$. Suppose Q is a 2×2 unitary and let $|\beta\rangle = Q|0\rangle$ and $|\beta^\perp\rangle = Q|1\rangle$. There exist 2×2 unitary matrices P_0, P_1 such that

$$I \otimes I \otimes |\beta\rangle\langle\beta| + P_0 \otimes P_1 \otimes |\beta^\perp\rangle\langle\beta^\perp| = CC(\text{Diag}(u_0, u_1))$$

if and only if $u_0 = 1$ and $u_1 = 1$.

Proof. Forward direction: case-split on the components a, b of $|\beta\rangle$. If $a = 0$ then $|\beta\rangle\langle\beta| = |1\rangle\langle 1|$ and $|\beta^\perp\rangle\langle\beta^\perp| = |0\rangle\langle 0|$; extracting diagonal entries of $CC(\text{Diag}(u_0, u_1))$ forces $u_0 = 1$ and $u_1 = 1$. The case $b = 0$ is symmetric. If both $a \neq 0$ and $b \neq 0$, multiply both sides by $|1\rangle\langle 1| \otimes |\beta\rangle\langle\beta|$; the $|\beta^\perp\rangle$ term vanishes by orthogonality, yielding $\text{Diag}(u_0, u_1)|\beta\rangle = |\beta\rangle$, so $u_0 = 1$ and $u_1 = 1$ by cancellation.

Reverse direction: take $P_0 = P_1 = I$ and use $Q|0\rangle\langle 0|Q^\dagger + Q|1\rangle\langle 1|Q^\dagger = I$. $\square$

Lemma 6. Suppose u_0, u_1 are complex numbers with $|u_0| = |u_1| = 1$. There exist 4×4 unitary matrices V_1, V_2, V_3, V_4 and 2×2 unitary matrices P_0, P_1 , where $V_1 = |0\rangle\langle 0| \otimes P_0 + |1\rangle\langle 1| \otimes P_1$, such that

$$(V_1)_{AC} \cdot (V_2)_{BC} \cdot (V_3)_{AC} \cdot (V_4)_{BC} = CC(\text{Diag}(u_0, u_1))$$

if and only if either $u_0 = u_1$ or $u_0 u_1 = 1$.

Proof. Forward direction: decompose $CC(\text{Diag}(u_0, u_1))$ as $|0\rangle\langle 0| \otimes I_4 + |1\rangle\langle 1| \otimes C(\text{Diag}(u_0, u_1))$. Since V_1 is controlled on qubit A , apply Lemma A.27 to the alternating AC/BC product to extract 2×2 unitaries Q_0, Q_1 such that the three-factor product $V_1 \cdot V_2 \cdot V_3$ decomposes blockwise. Eliminate V_4 to obtain $(I \otimes P_1)V_2(I \otimes Q_1) = C(\text{Diag}(u_0, u_1)) \cdot ((I \otimes P_0)V_2(I \otimes Q_0))^\dagger$. Apply the spectral theorem to $Q_1 Q_0^\dagger$ to obtain a diagonal matrix D , then invoke Lemma 3.3 on the resulting eigenvalue condition.

Reverse direction: if $u_0 = u_1$, take $V_1 = I_4$, $V_2 = \text{swap}$, $V_3 = C(\text{Diag}(1, u_1))$, $V_4 = \text{swap}$. If $u_0 u_1 = 1$, write $u_1 = e^{i\theta}$, set $u = e^{i\theta/2}$, $P = \text{Diag}(u^{-1}, u)$, and construct $V_1 = V_3 = C(P)$ on AC , $V_2 = |0\rangle\langle 0| \otimes \sigma_x + |1\rangle\langle 1| \otimes I$ on BC , $V_4 = V_2^\dagger$. $\square$

Lemma 7. Suppose u_0, u_1 are complex numbers with $|u_0| = |u_1| = 1$. There exist 4×4 unitary matrices V_1, V_2, V_3, V_4 and 2×2 unitary matrices P_0, P_1 , where $V_4 = |0\rangle\langle 0| \otimes P_0 + |1\rangle\langle 1| \otimes P_1$, such that

$$(V_1)_{AC} \cdot (V_2)_{BC} \cdot (V_3)_{AC} \cdot (V_4)_{BC} = CC(\text{Diag}(u_0, u_1))$$

if and only if either $u_0 = u_1$ or $u_0 u_1 = 1$.

Proof. Follows from Lemma 4.3 by exchanging the roles of qubits A and B and taking the conjugate transpose of the entire product. Given a decomposition with V_1 controlled, take adjoints of all factors and reverse their order; the controlled structure migrates from V_1 to V_4 . The condition $u_0 = u_1$ or $u_0 u_1 = 1$ is preserved under conjugation since $|u_0^*| = |u_0|$ and $u_0^* u_1^* = (u_0 u_1)^*$. $\square$

0.4 Section 5: The first main lemma

Lemma 8. *Suppose u_0, u_1 are complex numbers with $|u_0| = |u_1| = 1$. There exist 2-qubit unitaries U_1, U_2, U_3, U_4 such that $U_1^{BC} U_2^{AC} U_3^{AB} U_4^{BC} = CC(\text{Diag}(u_0, u_1))$ if and only if either $u_0 = u_1$ or $u_0 u_1 = 1$.*

Proof. (Forward direction.) Rearrange to isolate $U_2^{AC} U_3^{AB} = (U_1^{BC})^\dagger CC(\text{Diag}(u_0, u_1)) (U_4^{BC})^\dagger$. Each of $(U_1^{BC})^\dagger$, $CC(\text{Diag}(u_0, u_1))$, and $(U_4^{BC})^\dagger$ commutes with $\text{Diag}(u_0, u_1) \otimes I_{BC}$, so $U_2^{AC} U_3^{AB}$ commutes with $\text{Diag}(u_0, u_1) \otimes I_2 \otimes I_2$. By Lemma 1, either $u_0 = u_1$ (done), or $U_2^{AC} U_3^{AB} = |0\rangle\langle 0| \otimes V_0 + |1\rangle\langle 1| \otimes V_1$ for 4×4 unitaries V_0, V_1 . By Lemma A.24, this refines to $U_2^{AC} U_3^{AB} = |0\rangle\langle 0| \otimes P_0 \otimes Q_0 + |1\rangle\langle 1| \otimes P_1 \otimes Q_1$ for 2×2 unitaries P_0, Q_0, P_1, Q_1 . Substituting back gives $CC(\text{Diag}(u_0, u_1)) = |0\rangle\langle 0| \otimes U_1(P_0 \otimes Q_0)U_4 + |1\rangle\langle 1| \otimes U_1(P_1 \otimes Q_1)U_4$. By Lemma 4, either $u_0 = u_1$ or $u_0 u_1 = 1$.

(Backward direction, case $u_0 = u_1$.) Set $U = C(\text{Diag}(1, u_1))$ and verify $I^{BC} I^{AC} U^{AB} I^{BC} = CC(\text{Diag}(u_1, u_1))$ by direct computation.

(Backward direction, case $u_0 u_1 = 1$.) Define $V = \text{Diag}(1, 1, 1, u_1)$ and $W = \text{Diag}(1, 1, 1, u_0)$, and let U be the permutation matrix swapping the second and fourth basis vectors. Verify $U^{BC} V^{AC} W^{AB} U^{BC} = CC(\text{Diag}(u_0, u_1))$ by direct computation, using $u_0 u_1 = 1$ to simplify diagonal entries. $\square$

0.5 Section 6: The second main lemma

Lemma 9. *(Case analysis of a unitary.) For a 2-qubit unitary V , either $\exists |x\rangle : V(|x\rangle \otimes |0\rangle)$ is entangled, or $\exists |\psi\rangle : \forall |x\rangle : \exists |z\rangle : V(|x\rangle \otimes |0\rangle) = |z\rangle \otimes |\psi\rangle$, or $\exists |\psi\rangle : \forall |x\rangle : \exists |z\rangle : V(|x\rangle \otimes |0\rangle) = |\psi\rangle \otimes |z\rangle$.*

Proof. Either $\exists |x\rangle$ such that $V(|x\rangle \otimes |0\rangle)$ is entangled, or $\forall |x\rangle$, $V(|x\rangle \otimes |0\rangle)$ is not entangled and hence is a tensor product. In the second case, apply Lemma A.23 to distinguish two sub-cases: either the second factor is fixed ($\exists |\psi\rangle : \forall |x\rangle : \exists |z\rangle : V(|x\rangle \otimes |0\rangle) = |z\rangle \otimes |\psi\rangle$) or the first factor is fixed ($\exists |\psi\rangle : \forall |x\rangle : \exists |z\rangle : V(|x\rangle \otimes |0\rangle) = |\psi\rangle \otimes |z\rangle$). $\square$

Lemma 10. *Suppose u_0, u_1 are complex numbers such that $|u_0| = |u_1| = 1$. For 2-qubit unitaries U_1, W_2, V_3, U_4 , if*

$$U_1^{AC} W_2^{BC} V_3^{AC} U_4^{BC} = CC(\text{Diag}(u_0, u_1)),$$

$V_3(|0\rangle \otimes |0\rangle) = |0\rangle \otimes |0\rangle$, and for any $|x_A\rangle : U_1^{AC}(|x_A\rangle \otimes |0_B\rangle \otimes |0_C\rangle) = U_4^{BC\dagger} V_3^{AC\dagger}(|x_A\rangle \otimes |0_B\rangle \otimes |0_C\rangle)$, then either $u_0 = u_1$ or $u_0 u_1 = 1$ or there exist 2-qubit unitaries W_1, W_3, W_4 and a 1-qubit unitary P_3 such that

$$U_1^{AC} W_2^{BC} V_3^{AC} U_4^{BC} = W_1^{AC} W_2^{BC} W_3^{AC} W_4^{BC}$$

and $W_3 = I \otimes |0\rangle\langle 0| + P_3 \otimes |1\rangle\langle 1|$.

Proof. Apply Lemma 9 to $V_3^\dagger$ for a three-case analysis.

Case 1 (entangled): Use swap-based manipulation (Lemmas A.10, A.12) to convert the AC-gate identity to a BC-gate form. Then Lemma A.19 gives $U_4^\dagger = |0\rangle\langle 0| \otimes Q_0 + |1\rangle\langle 1| \otimes Q_1$. Conclude $u_0 = u_1$ or $u_0 u_1 = 1$ via Lemma 7.

Case 2 ($V_3^\dagger(|x\rangle \otimes |0\rangle) = |z\rangle \otimes |\psi\rangle$): Lemma A.31 directly gives the decomposition with $W_3 = I \otimes |0\rangle\langle 0| + P_3 \otimes |1\rangle\langle 1|$.

Case 3 ($V_3^\dagger(|x\rangle \otimes |0\rangle) = |\psi\rangle \otimes (P_0|x\rangle)$): Use Lemma A.25 to extract P_0 . Derive $\forall |x\rangle : \exists |w\rangle : U_4^\dagger(|0\rangle \otimes (P_0|x\rangle)) = |0\rangle \otimes |w\rangle$ via Lemma A.22. Then Lemma A.17 gives $U_4^\dagger = |0\rangle\langle 0| \otimes Q_0 + |1\rangle\langle 1| \otimes Q_1$. Conclude via Lemma 7. $\square$

Lemma 11. Suppose u_0, u_1 are complex numbers such that $|u_0| = |u_1| = 1$. For 2-qubit unitaries V_1, V_2, V_3, V_4 , if

$$V_1^{AC} V_2^{BC} V_3^{AC} V_4^{BC} = CC(\text{Diag}(u_0, u_1)),$$

$\exists |\psi\rangle : \forall |x\rangle : \exists |z\rangle : V_2(|x\rangle \otimes |0\rangle) = |z\rangle \otimes |\psi\rangle$, and $V_3(|0\rangle \otimes |0\rangle) = |0\rangle \otimes |0\rangle$, then either $u_0 = u_1$ or $u_0 u_1 = 1$ or there exist 2-qubit unitaries W_1, W_2, W_3, W_4 and 1-qubit unitaries P_1, P_2, P_3, P_4, Q such that

$$\begin{aligned} W_1^{AC} W_2^{BC} W_3^{AC} W_4^{BC} &= CC(\text{Diag}(u_0, u_1)), \\ W_1 &= I \otimes |\beta\rangle\langle 0| + P_1 \otimes |\beta^\perp\rangle\langle 1|, \\ W_2 &= I \otimes |0\rangle\langle 0| + P_2 \otimes |1\rangle\langle 1|, \\ W_3 &= I \otimes |0\rangle\langle 0| + P_3 \otimes |1\rangle\langle 1|, \\ W_4 &= I \otimes |0\rangle\langle \beta| + P_4 \otimes |1\rangle\langle \beta^\perp|, \end{aligned}$$

where $|\beta\rangle = Q|0\rangle$ and $|\beta^\perp\rangle = Q|1\rangle$.

Proof. Use Lemma A.30 on the V_2 assumption to rewrite the product as $U_1^{AC} W_2^{BC} V_3^{AC} U_4^{BC}$ with $W_2 = I \otimes |0\rangle\langle 0| + P_2 \otimes |1\rangle\langle 1|$. From $W_2(|0\rangle \otimes |0\rangle) = |0\rangle \otimes |0\rangle$ and Lemma A.29, derive $\forall |x_A\rangle : U_1^{AC}(|x_A\rangle \otimes |0_B\rangle \otimes |0_C\rangle) = U_4^{BC\dagger} V_3^{AC\dagger}(|x_A\rangle \otimes |0_B\rangle \otimes |0_C\rangle)$. Apply Lemma 10 to get a three-way disjunction.

In the third case, use Lemma A.28 and A.22 to derive $\forall |z\rangle : W_4^\dagger(|z\rangle \otimes |0\rangle) = |z\rangle \otimes |\beta\rangle$ for a fixed $|\beta\rangle$ (via Lemma A.26). Define $Q = |\beta\rangle\langle 0| + |\beta^\perp\rangle\langle 1|$ and verify Q is unitary. Show $W_4 \cdot (I \otimes Q)(|z\rangle \otimes |0\rangle) = |z\rangle \otimes |0\rangle$; apply Lemma A.18 to derive $W_4 = I \otimes |0\rangle\langle \beta| + P_4 \otimes |1\rangle\langle \beta^\perp|$. Similarly derive $W_1 = I \otimes |\beta\rangle\langle 0| + P_1 \otimes |\beta^\perp\rangle\langle 1|$ using Lemma A.29 and Lemma A.18. $\square$

Lemma 12. (The second main lemma.) Suppose u_0, u_1 are complex numbers such that $|u_0| = |u_1| = 1$. There exist 2-qubit unitaries U_1, U_2, U_3, U_4 such that

$$U_1^{AC} U_2^{BC} U_3^{AC} U_4^{BC} = CC(\text{Diag}(u_0, u_1))$$

if and only if either $u_0 = u_1$ or $u_0 u_1 = 1$.

Proof. (Forward direction.) Use Lemma A.32 to obtain V_1, V_2, V_3, V_4 with $V_3(|0\rangle \otimes |0\rangle) = |0\rangle \otimes |0\rangle$ and $V_1^{AC} V_2^{BC} V_3^{AC} V_4^{BC} = CC(\text{Diag}(u_0, u_1))$. Apply Lemma A.28 to derive $V_1^{AC} V_2^{BC}(|0_A\rangle \otimes |x_B\rangle \otimes |0_C\rangle) = V_4^{BC\dagger}(|0_A\rangle \otimes |x_B\rangle \otimes |0_C\rangle)$. Three-case analysis on V_2 via Lemma 9.

Case 1 (entangled): Lemma A.19 gives $V_1 = |0\rangle\langle 0| \otimes P_0 + |1\rangle\langle 1| \otimes P_1$. Conclude via Lemma 6.

Case 2 ($V_2(|x\rangle \otimes |0\rangle) = |\psi\rangle \otimes |z\rangle$): Lemma A.33 gives the same block-diagonal form for V_1 . Conclude via Lemma 6.

Case 3 ($V_2(|x\rangle \otimes |0\rangle) = |z\rangle \otimes |\psi\rangle$): Apply Lemma 11 to get the structured decomposition with $W_1, \dots, W_4$. Compute $CC(\text{Diag}(u_0, u_1)) = I \otimes I \otimes |\beta\rangle\langle \beta| + (P_1 P_3) \otimes (P_2 P_4) \otimes |\beta^\perp\rangle\langle \beta^\perp|$. Conclude $u_0 = u_1$ via Lemma 5.

(Backward direction.) Use the right-to-left direction of Lemma 6. $\square$

0.6 Section 7: The main theorem

Throughout this section, for complex numbers u_0, u_1 with $|u_0| = |u_1| = 1$, we define $R(u_0, u_1) = \{(u_0, u_1), (1, u_0^* u_1)\}$.

Lemma 13. *Suppose u_0, u_1 are complex numbers with $|u_0| = |u_1| = 1$. For a 2-qubit unitary W and a 3-qubit unitary U , if $CC(\text{Diag}(u_0, u_1)) = W^{AB} \cdot U$, then there exists a 2-qubit unitary V such that $CC(\text{Diag}(1, u_0^* u_1)) = V^{AB} \cdot U$.*

Proof. Set $V = C(\text{Diag}(1, u_0^*)) \cdot W$. Then V is a 2-qubit unitary. Expand $V^{AB} \cdot U$ using the hypothesis $W^{AB} \cdot U = CC(\text{Diag}(u_0, u_1))$ to obtain $V^{AB} \cdot U = C(\text{Diag}(1, u_0^*))^{AB} \cdot CC(\text{Diag}(u_0, u_1))$. Both factors are diagonal in the computational basis, so the product is verified entry-by-entry: the diagonal entries combine to give $CC(\text{Diag}(1, u_0^* u_1))$. $\square$

Lemma 14. *Suppose u_0, u_1 are complex numbers with $|u_0| = |u_1| = 1$. If there exists a product of at most four elements of $G_2 \setminus G_1$ and any number of elements of G_1 that equals $CC(\text{Diag}(u_0, u_1))$, then either:*

1. *there exist 2-qubit unitaries U_1, U_2, U_3, U_4 and $(u_2, u_3) \in R(u_0, u_1)$ such that $U_1^{BC} U_2^{AC} U_3^{AB} U_4^{BC} = CC(\text{Diag}(u_2, u_3))$, or*
2. *there exist 2-qubit unitaries U_1, U_2, U_3, U_4 and $(u_2, u_3) \in R(u_0, u_1)$ such that $U_1^{AC} U_2^{BC} U_3^{AC} U_4^{BC} = CC(\text{Diag}(u_2, u_3))$.*

Proof. The proof proceeds in four steps.

(Step 1.) Each element of G_1 can be absorbed into an adjacent element of $G_2 \setminus G_1$, reducing to at most four factors from $G_2 \setminus G_1$.

(Step 2.) By padding with identity factors if fewer than four $G_2 \setminus G_1$ factors remain, write the product as exactly four canonical factors $V_1 V_2 V_3 V_4$, where each V_i is of the form U^{XY} for some pair XY .

(Step 3.) Using the swap conjugation identities (Lemma A.12), reduce to the case where V_4 has label BC . This may change the diagonal parameters from (u_0, u_1) to $(1, u_0^* u_1)$ via Lemma 13, so the new parameters $(u_2, u_3) \in R(u_0, u_1)$.

(Step 4.) Using Lemma A.13 and the swap conjugation identities, case-analyse over the labels of V_1, V_2, V_3 to reduce to one of the two canonical forms stated in the conclusion. $\square$

Lemma 15. *Suppose u_0, u_1 are complex numbers with $|u_0| = |u_1| = 1$. Suppose $(u_2, u_3) \in R(u_0, u_1)$. If $u_2 = u_3$ or $u_2 u_3 = 1$, then $u_0 = u_1$ or $u_0 u_1 = 1$.*

Proof. Since $(u_2, u_3) \in R(u_0, u_1)$, either $(u_2, u_3) = (u_0, u_1)$ or $(u_2, u_3) = (1, u_0^* u_1)$. Cross with the hypothesis $u_2 = u_3$ or $u_2 u_3 = 1$ to obtain four subcases. In the case $(u_2, u_3) = (u_0, u_1)$, the conclusion holds immediately. In the case $(u_2, u_3) = (1, u_0^* u_1)$ with $u_2 = u_3$, we get $u_0^* u_1 = 1$, so $u_0 u_1 = |u_0|^2 u_0 u_1 / u_0 u_1$; using $|u_0| = 1$ gives $u_0 = u_1$. In the case $(u_2, u_3) = (1, u_0^* u_1)$ with $u_2 u_3 = 1$, we get $u_0^* u_1 = 1$, hence $u_0 = u_1$. $\square$

Theorem 16. *Suppose u_0, u_1 are complex numbers with $|u_0| = |u_1| = 1$. There exists a product of at most four elements of $G_2 \setminus G_1$ and any number of elements of G_1 that equals $CC(\text{Diag}(u_0, u_1))$ if and only if either $u_0 = u_1$ or $u_0 u_1 = 1$.*

Proof. (Forward direction.) By Lemma 14, the hypothesis reduces to one of two canonical forms with parameters $(u_2, u_3) \in R(u_0, u_1)$. In form (1), $U_1^{BC} U_2^{AC} U_3^{AB} U_4^{BC} = CC(\text{Diag}(u_2, u_3))$, so by Lemma 8 either $u_2 = u_3$ or $u_2 u_3 = 1$. In form (2), $U_1^{AC} U_2^{BC} U_3^{AC} U_4^{BC} = CC(\text{Diag}(u_2, u_3))$,

so by Lemma 12 either $u_2 = u_3$ or $u_2 u_3 = 1$. In either case, Lemma 15 lifts the conclusion to $u_0 = u_1$ or $u_0 u_1 = 1$.

(Backward direction.) If $u_0 = u_1$ or $u_0 u_1 = 1$, Lemma 8 (backward) provides a decomposition $U_1^{BC} U_2^{AC} U_3^{AB} U_4^{BC} = CC(\text{Diag}(u_0, u_1))$, each factor being an element of G_2 . $\square$

Corollary 17. *For a 1-qubit unitary U , there exists a product of at most four elements of $G_2 \setminus G_1$ and any number of elements of G_1 that equals $CC(U)$ if and only if either the eigenvalues of U are equal or $\det(U) = 1$.*

Proof. By the spectral theorem (Theorem A.3), write $U = V \text{Diag}(u_0, u_1) V^\dagger$ for a unitary V and eigenvalues u_0, u_1 with $|u_0| = |u_1| = 1$. Then $CC(U) = (I \otimes I \otimes V) CC(\text{Diag}(u_0, u_1)) (I \otimes I \otimes V^\dagger)$. Since $I \otimes I \otimes V \in G_1$, conjugating by it does not change the number of $G_2 \setminus G_1$ factors needed. Apply Theorem 16 to $CC(\text{Diag}(u_0, u_1))$ to conclude: the decomposition exists if and only if $u_0 = u_1$ or $u_0 u_1 = 1$. The condition $u_0 = u_1$ is equivalent to the eigenvalues being equal, and $u_0 u_1 = \det(U) = 1$. $\square$

0.7 Optimal implementation of Toffoli

Lemma 18 (Five-gate construction). *The Toffoli gate has an exact decomposition into five two-qubit gates.*

Proof. Let $V^2 = X$. The controlled- V , controlled- $V^\dagger$, and CNOT construction is verified on all eight computational basis states. $\square$

Lemma 19 (Four-gate lower bound). *No exact decomposition of Toffoli uses at most four two-qubit gates.*

Proof. Apply Corollary 17 to $U = X$. The eigenvalues of X are distinct and $\det X = -1$, so neither condition permitting a four-gate decomposition holds. Shorter decompositions are padded by identity gates. $\square$

Theorem 20 (Five two-qubit gates are necessary and sufficient). *Five two-qubit gates are necessary and sufficient to implement a Toffoli gate exactly.*

Proof. Combine the explicit five-gate construction with the impossibility of every decomposition of length at most four. $\square$